Abstract

Security of communications is a major requirement for Mobile Ad hoc NETworks (MANETs) since they use wireless channel for communications which can be easily tapped, and physical capture of MANET nodes is also quite easy. From the point of view of providing security in MANETs, there are basically two types of MANETs, viz., authoritarian MANETs, in which there exist one or more authorities who decide the members of the network, and self-organized MANETs, in which there is no such authority. Ensuring security of communications in the MANETs is a challenging task due to the resource constraints and infrastructure-less nature of these networks, and the limited physical security of MANET nodes. Attacks on security in a MANET can be launched by either the external attackers which are not legitimate members of the MANET or the internal attackers which are compromised members of the MANET and which can hold some valid security credentials or both. Key management and authentication protocols (KM-APs) play an important role in preventing the external attackers in a MANET. However, in order to prevent the internal attackers, an intrusion detection system (IDS) is essential. The routing protocols running in the network layer of a MANET are most vulnerable to the internal attackers, especially to the attackers which launch packet dropping attack during data packet forwarding in the MANET. For an authoritarian MANET, an arbitrated KM-AP protocol is perfectly suitable, where trusts among network members are co-ordinated by a trusted authority. Moreover, due to the resource constraints of a MANET, symmetric key management protocols are more efficient than the public

key management protocols in authoritarian MANETs. The existing arbitrated symmetric key management protocols in MANETs, that do not use any authentication server inside the network are susceptible to identity impersonation attack during shared key establishments. On the other hand, the existing server co-ordinated arbitrated symmetric key management protocols in MANETs do not differentiate the role of a membership granting server (MGS) from the role of an authentication server, and so both are kept inside the network. However, keeping the MGS outside the network is more secure than keeping it inside the network for a MANET. Also, the use of a single authentication server inside the network cannot ensure robustness against authentication server compromise. In self-organized MANETs, public key management is more preferable over symmetric key management, since the distribution of public keys does not require a pre-established secure channel. The main problem for the existing self-organized public key management protocols in MANETs is associated with the use of large size certificate chains. Besides, the proactive certificate chaining based approaches require each member of a MANET to maintain an updated view of the trust graph of the entire network, which is highly resource consuming. Maintaining a hierarchy of trust relationships among members of a MANET is also problematic for the same reason. Evaluating the strength of different alternative trust chains and restricting the length of a trust chain used for public key verification is also important for enhancing the security of self-organized public key management protocols. The existing network layer IDS protocols in MANETs that try to defend against packet dropping attack use either a reputation based or an incentive based approach. The reputation based approaches are more effective against malicious principals than the incentive based approaches. The major problem associated with the existing reputation based IDS protocols is that they do not consider the protocol soundness issue in their design objectives. Besides, most of the existing protocols incorporate no mechanism to fight against colluding principals. Also, an IDS protocol in MANETs should incorporate some secure and efficient mechanism to authenticate the control packets used by it. In order to mitigate the above mentioned problems in MANETs, we have

proposed new models and designed novel security protocols in this thesis that can enhance the security of communications in MANETs at lesser or comparable cost. First, in order to perform security analysis of KM-AP protocols, we have extended the well known strand space verification model to overcome some of its limitations. Second, we have proposed a model for the study of membership of principals in MANETs with a view to utilize the concept for analyzing the applicability and the performance of KM-AP protocols in different types of MANETs. Third and fourth, we have proposed two novel KM-AP protocols, SEAP and CLPKM, applicable in two different types of MANET scenarios. The SEAP protocol is an arbitrated symmetric key management protocol designed to work in an authoritarian MANET, whereas the CLPKM protocol is a self-organized public key management protocol designed for self-organized MANETs. Fifth, we have designed a novel reputation based network layer IDS protocol, named EVAACK protocol, for the detection of packet dropping misbehavior in MANETs. All of the three proposed protocols try to overcome the limitations of the existing approaches in their respective categories. We have provided rigorous mathematical proofs for the security properties of the proposed protocols. Performance of the proposed protocols have been compared with those of the other existing similar approaches using simulations in the QualNet simulator. In addition, we have also implemented the proposed SEAP and CLPKM protocols on a real MANET testbed to test their performances in real environments. The analytical, simulation and experimentation results confirm the effectiveness of the proposed schemes.